REMARKS

The above amendments to the specification, claims and abstract have been made to place the application in proper U.S. format and to conform with proper grammatical and idiomatic English. None of the amendments herein are made for reasons related to patentability. No new matter has been added.

Attached hereto is a marked-up version of the changes made to the specification and claims by the current amendment. The attached page is captioned "**Version with markings to show changes made**".

In the unlikely event that the transmittal letter is separated from this document and the Patent Office determines that an extension and/or other relief is required, applicant petitions for any required relief including extensions of time and authorizes the Commissioner to charge the cost of such petitions and/or other fees due in connection with the filing of this document to **Deposit Account No. 03-1952** referencing docket no. 44912-20050.00. However, the Commissioner is not authorized to charge the cost of the issue fee to the Deposit Account.

Respectfully submitted,

Dated: September 19, 2001

By: _____
Spivak, Kevin R.
Registration No. 43,148

Morrison & Foerster LLP
2000 Pennsylvania Avenue, N.W.
Washington, D.C. 20006-1888
Telephone: (202) 887-6924
Facsimile: (202) 263-8396

VERSION WITH MARKINGS TO SHOW CHANGES MADE

For the convenience of the Examiner, the changes made are shown below with deleted text in strikethrough and added text in underline.

In the Specification:

Page 1 before the first paragraph, has been amended to delete the following:

~~Description~~

Page 1, line 3, has been amended to include the following Title:

SYSTEM AND METHOD FOR CHECKING THE AUTHENTICITY OF AN APPLICATION IN A TELECOMMUNICATIONS NETWORK

Page 1, before the first paragraph, has been amended to include the following heading and insert:

Claim for Priority

This application claims priority to International Application No. PCT/DE00/00827 which was published in the German language on March 19, 1999.

Page 1, between lines 7 and 8, has been amended to include the following heading:

TECHNICAL FIELD OF THE INVENTION

Paragraph beginning on line 8 of page 1 has been amended as follows:

The present invention relates to a method for checking the authenticity of a manager application in a telecommunications management network operating system

~~(TMN-OS) according to the precharacterizing clause of the method claim 1~~, and to an associated network element ~~according to the precharacterizing clause of the apparatus claim 5~~.

Page 1, between lines 15 and 16, has been amended to include the following heading:

BACKGROUND OF THE INVENTION

Paragraph beginning on line 16 of page 1 has been amended as follows:

Switching devices, ~~which are~~ also referred to as network elements, are used as nodes in a telecommunications network in order to coordinate the information flow in such networks. The network elements are managed by a specific operating system, the TMN-OS. For this purpose, they are connected together with the operating system to a specific management network, which is referred to as the telecommunications management network (TMN)~~;~~. ~~the~~ The network elements are managed by the operating system TMN-OS communicating with the network elements via the TMN.

Paragraph beginning on line 1 of page 2 has been amended as follows:

At the start of or during the handling of a communication protocol, it is possible to provide for the authenticity of a manager application to be checked by a network element. To do this, the manager application ~~which wishes~~ desiring to set up a link to the network element must prove, i.e. authenticate, that it is ~~that~~ the manager application which it claims to be.

Paragraph beginning on line 27 of page 2 has been amended as follows:

In addition to these various protocol-specific authentication data items, a number of checking mechanisms, which are referred to as authentication types, are generally provided for each communication protocol, for carrying out the authentication check as shown in Figure 2. ~~; according~~ According to Figure 2, for the Q3 communication protocol for example, these are a simple password mechanism, a replay protected password mechanism, a pure identification, or a challenge and response method.

Paragraph beginning on line 1 of page 3 has been amended as follows:

This means that, before each authentication check, one of the ~~respectively~~ available authentication types must be selected to carry out that particular authentication check.

Paragraph beginning on line 6 of page 3 has been amended as follows:

Conventionally, there are ~~therefore~~ various software programs, which are referred to as protocol-specific applications, for each communication protocol (and in some cases these even have different operator interfaces (MML, Q3)) for managing the authentication data and the authentication types.

Page 3, between lines 12 and 13, has been amended to include the following heading and paragraphs:

SUMMARY OF THE INVENTION

In one embodiment of the invention, there is a method for checking the authenticity of a manager application in a telecommunications management network operating system (TMN-

OS). The method includes, for example, transmitting a communication-protocol-specific authentication data from the manager application via a telecommunication management network (TMN) to a network element while handling a communication protocol, the communication protocol-specific authentication data used by the network element to check the authenticity of the manager application, and checking the authenticity of the manager application by comparing the communication protocol-specific authentication data with predetermined authentication data, wherein authentication checking is carried out centrally in an authenticity checking device for various communication protocols, and authentication data for the communication protocols used are stored centrally in an authentication databank.

In another aspect of the invention, there is a method that includes managing the central authentication databank by a dedicated communication protocol.

In another aspect of the invention, the method includes the communication protocols Q3, FTAM, FTP or MML protocol.

In yet another aspect of the invention, the method includes authentication checking for each individual communication protocol is carried out centrally in the authenticity checking device using different authentication types.

In one embodiment of the invention, there is a network element in a telecommunications network, the network element managed by a telecommunications management network operating system (TMN-OS) via a telecommunications management network (TMN). The method includes, for example, at least one agent application for receiving communication-protocol-specific authentication data via the TMN from an associated manager application in the TMN-OS, the authentication data used to check the authenticity of the associated manager application, and an authenticity checking device to receive the communication protocol-specific

authentication data from the agent application and to check the authenticity of the manager application by comparing the communication protocol-specific authentication data with predetermined authentication data, wherein the authenticity checking device carries out the authentication checking centrally for various communication protocols, and the authentication data for the communication protocols used are stored centrally in an authentication databank.

In another aspect of the invention, the method includes the network element wherein the network element has a management device which manages the central authentication databank.

In another aspect of the invention, the method includes the network element wherein the management device is coupled to the TMN via a dedicated agent application and is controlled by the TMN-OS.

Brief Description of the Drawings

The following text includes a detailed description of an exemplary embodiment of the invention, with reference to the attached figures.

Figure 1 shows a TMN as a connecting network between a TMN-OS and a network element according to the present invention.

Figure 2 shows a tabular association between communication protocols and respective possible authentication types.

Page 3, before the paragraph beginning on line 13, the following heading has been inserted:

Detailed Description of the Preferred Embodiments

Paragraph beginning on line 13 of page 3 has been amended as follows:

The ~~object of the~~ method ~~is to~~ provides a ~~method which is~~ simpler method than the conventional method for a network element to check the authenticity of a manager application and to provide a network element which is suitable for this purpose, in which method and network element the various protocol-specific applications for managing the authentication data are superfluous.

Paragraph beginning on line 21 of page 3 has been deleted in its entirety.

Paragraph beginning on line 26 of page 3 has been amended as follows:

According to ~~patent claims 1 and 5, the object is achieved in particular in that~~ the invention, the authentication check is carried out centrally in an authentication checking device in the network element for various manager applications, that is ~~to say~~ for various communication protocols.~~, and in that the~~ The authentication checking device accesses an authentication databank in which the various authentication data for ~~all~~ the communication protocols used are stored centrally.

Paragraph beginning on line 31 of page 4 has been amended as follows:

In a preferred embodiment ~~development~~ of the checking method according to the invention, ~~the step of~~ authentication checking is carried out centrally in the network element not only for each individual communication protocol, but also for different authentication types. This centralization also saves costly communication-protocol-specific individual solutions.

Paragraph beginning on line 1 of page 5 has been amended as follows:

Finally, for the network element designed for carrying out the method, it is advantageous for the central authentication databank to be managed by a management device which is controlled by the TMN-OS via a dedicated agent application within the network element. In addition to saving communication-protocol-specific individual solutions for managing the communication-protocol-specific authentication data, this ~~development furthermore~~ embodiment allows decoupling of telecommunication-specific communication and management communication between the TMN-OS and the network element.

Paragraph beginning on line 10 of page 6 has been deleted in its entirety.

Paragraph beginning on line 14 of page 6 has been deleted in its entirety.

Paragraph beginning on line 18 of page 6 has been deleted in its entirety.

Paragraph beginning on line 22 of page 6 has been amended as follows:

A network element in a communications network is managed by a telecommunications management network operating system (TMN-OS). Figure 1 shows the coupling of the network element to the TMN-OS via a TMN that is required for this purpose. The TMN-OS has a large number of manager applications 50, 60...100, which are implemented either in hardware, ~~but normally~~ or preferably in software. One or more of these manager applications can then run on a computer.

Paragraph beginning on line 32 of page 6 has been amended as follows:

The network element in each case has a corresponding mating part, which is referred to as an agent application 55, 65...105, in the TMN-OS for each manager application. Using these agent applications, the network element communicates via the TMN with the manager applications 50, 60...100 in the TMN-OS. Each manager application communicates with its associated agent application in the form of an individual communication protocol. In this case, the following ~~constellations~~ associations are possible, according to Figure 1: the File Transfer Access Management (FTAM) manager application 50 communicates with the FTAM agent application 55; the File Transfer Protocol (FTP) manager application 60 communicates with the FTP agent application 65; the Man Machine Language (MML) manager application 70 communicates with the MML agent application 75; and the Q3 manager applications 80, 100 communicate with the Q3 agent applications 85, 105 in the network element.

Paragraph beginning on line 24 of page 6 has been amended as follows:

In the course of the unilateral authentication check shown in Figure 1, a manager application 50, 60...100 which wishes to set up a connection to the network element initially sets up the protocol elements required for carrying out the authentication check. The check is carried out as a function of its communication protocol, its initiators and a selected authentication type, and sends these to the network element. These protocol elements are then received and evaluated by the network element. During the evaluation process, the authentication data required for carrying out the authentication check is, in particular, filtered out of the protocol elements. Each of the communication protocols

used, for example the FTAM, FTP, MML or Q3 communication protocol, ~~each~~ has its own dedicated authentication data.

Paragraph beginning on line 35 of page 7 has been amended as follows:

With regard to future communications between the TMN-OS and the network element, authentication data for a protocol which is to be used are initially stored in the central authentication databank 10. This is done in such a way that a Q3 manager application requests a Q3 management device 30 within the network element to enter the initiator "HUGO" in the central authentication databank 10, for example for future communication using the FTAM protocol, and such that this uses the "simple password mechanism" authentication type for authentication and such that its identification word is "ABCD1#".

Paragraph beginning on line 15 of page 9 has been amended as follows:

From the FTAM agent application 55 in the network element, it receives the information that the FTAM manager application 50 would like to set up a connection, with the manager application outputting "HUGO" as the initiator for the desired connection, and asserting that its identification word is "ABCD1#". The central authentication checking device 20 then compares ~~these~~ data with the original authentication data, already stored in the central authentication databank 10, for the FTAM communication protocol and the "HUGO" initiator. If there is a match, ~~and, if they match,~~ allows the connection is allowed to be set up.

Paragraph beginning on line 1 of page 10 has been amended as follows:

The central authentication checking device 20 carries out the authentication check, which is described by way of example for the FTAM communication protocol, in the same way for ~~all~~ the other communication protocols used. In this instance, in each individual case, it accesses the central authentication databank 10, in which the authentication data for ~~all~~ the communication protocols are stored.

In the Claims:

~~Patent Claims~~ **What is claimed is:**

1. (Amended) A method for checking the authenticity of a manager application ~~(50...100)~~ in a telecommunications management network operating system ~~TMN-OS by means of a network element which is managed by the TMN-OS via an intermediate TMN, having the following steps:~~**(TMN-OS), comprising:**

~~transmission of~~ **transmitting a** communication-protocol-specific authentication data from a **the** manager application ~~(50, 60...100) via the TMN to the~~ **via a telecommunication management network (TMN) to a** network element ~~in the course of~~ **while** handling a communication protocol, ~~in which case the~~ **the communication** protocol-specific authentication data ~~are required for~~ **used by** the network element to check the authenticity of the manager application~~(50, 60...100)~~; and

checking the authenticity of the manager application by ~~comparison of the received~~ **comparing the communication** protocol-specific authentication data with predetermined~~, stored~~ authentication data**, wherein**~~;~~

~~characterized in that~~

~~the step of~~

authentication checking is carried out centrally in an authenticity checking device ~~(20)~~ for various communication protocols~~;~~, and ~~in that~~

authentication data for ~~all~~ the communication protocols used are stored centrally in an authentication databank ~~(10)~~.

2. (Amended) The method as claimed in claim 1, ~~furthermore characterized by the following step:~~ **further comprising:**

~~management of~~ **managing** the central authentication databank ~~(10)~~ by ~~means of~~ a dedicated communication protocol.

3. (Amended) The method as claimed in claim 1 ~~or 2, characterized in that~~**, wherein** the communication protocols are a Q3, FTAM, FTP or MML protocol.

4. (Amended) The method as claimed in ~~one of claims 1 to 3, characterized in that the step of~~ **claim 1, wherein** authentication checking for each ~~individual~~ communication protocol is carried out centrally in the authenticity checking device using different authentication types.

5. (Amended) A network element in a telecommunications network, ~~in which case~~ the network element ~~is~~ managed by a telecommunications management network operating system ~~TMN-OS~~**(TMN-OS)** via a telecommunications management network ~~TMN, having~~**(TMN), comprising**:

at least one agent application ~~(55, 65...105)~~ for receiving communication-protocol-specific authentication data via the TMN from an associated manager application ~~(50, 60...100)~~ in the TMN-OS, ~~in which case~~ the authentication data ~~are required for checking~~ **used to check** the authenticity of the associated manager application; and

an authenticity checking device ~~(20), for receiving the~~ **to receive the communication** protocol-specific authentication data from the agent application and ~~for checking~~ **to check** the authenticity of the ~~management~~ **manager** application by ~~comparison of the~~ **comparing the**

communication protocol-specific authentication data with predetermined~~, stored~~ authentication data**, wherein**~~;~~

~~characterized in that~~

the authenticity checking device ~~(20)~~ carries out the authentication checking centrally for various communication protocols, and ~~in that~~

the authentication data for ~~all~~ the communication protocols used are stored centrally in an authentication databank ~~(10)~~.

6. (Amended) The network element as claimed in claim 5, ~~characterized in that said~~ **wherein the** network element ~~also~~ has a management device ~~(30)~~ which manages the central authentication databank ~~(10)~~.

7. (Amended) The network element as claimed in claim 6, ~~characterized in that~~ **wherein** the management device ~~(30)~~ is coupled to the TMN via a dedicated agent application ~~(105)~~ and is controlled by the TMN-OS.